DAVID L. ANDERSON (CABN 149604)
United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

ROBERT S. LEACH (CABN 196191)
JONAS LERMAN (CABN 274733)
Assistant United States Attorneys

1301 Clay Street, Suite 340S
Oakland, California 94612
Telephone: (510) 637-3918
Fax: (510) 637-3724
Email: robert.leach@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

IN THE MATTER OF THE SEARCH OF A RESIDENCE IN OAKLAND, CALIFORNIA	No. 4-19-70053 KAW UNITED STATES' REQUEST FOR REVIEW OF THE DUTY MAGISTRATE JUDGE'S DENIAL OF A SEARCH WARRANT APPLICATION Date: January 30, 2019 Time: 10:30 a.m. Duty Judge: The Honorable James Donato

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

INTRODUCTION

On January 10, 2019, without the benefit of briefing, Magistrate Judge Kandis A. Westmore, the duty magistrate, issued a published order denying a search warrant application relating to an active law enforcement investigation. The requested search warrant would have permitted law enforcement officers, while searching a residence, to compel certain individuals there (including two identified subjects) to press a finger to certain digital devices found in the residence to unlock them. This practice, often called "use of biometrics," has been approved by magistrates in this District, both before and after the Magistrate Judge's ruling. It also has been approved by the majority of other courts to have considered the issue.

The Magistrate Judge's order is wrong, and this Court should overrule it or, at a minimum, vacate it. Because applying a subject's fingerprint to a device is not "testimonial," compelling a person to do so does not violate the Fifth Amendment privilege against self-incrimination. Use of biometrics is no more a Fifth Amendment violation than a host of practices approved as constitutional by the Supreme Court and the Ninth Circuit, including fingerprinting, photographing a subject, obtaining a voice or handwriting exemplar, or extracting a blood sample.

The Magistrate Judge, based largely on her conclusion that use of biometrics is testimonial under the Fifth Amendment, concluded that the search warrant application also violated the Fourth Amendment. That aspect of the Magistrate Judge's ruling also requires reversal or vacatur. Because a valid search warrant implicitly carries with it the limited authority to briefly detain the occupants on, or in the immediate vicinity of, the premises while the search is being conducted, and because a valid warrant need not include all details about how agents will execute it, the proposed warrant satisfied the Fourth Amendment.

BACKGROUND

I. Background Regarding Biometrics

Apple, Samsung, and other companies produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called Touch ID. Apple also has a feature called Face ID, which allows certain

iPhones to be unlocked with the user's face. Once a user has set up the fingerprint or face sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or face, the device unlocks. For fingerprint features, most devices can be set up to recognize multiple prints, so that different prints, not necessarily from the same person, will unlock the device. If there is no sensor on the device, the device will not open with prints.

There are limits on the ability to use a fingerprint or thumbprint to unlock a device, which varies by manufacturer. For example, with Apple, the Touch ID feature only permits up to five attempts with a print before the device will require the user to enter a passcode. Furthermore, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a print alone. Similarly, Touch ID will not allow access if the device has been restarted or was off and has been turned on, if the device has received a remote lock command, or if five attempts to match a print have been unsuccessful. Other brands have similar restrictions.

II. The Government's Investigation

The government is investigating possible extortion, in violation of 18 U.S.C. § 875(d), involving the use of a social media platform.

On January 3, 2019, the government submitted an application for a warrant to search a residence in Oakland ("Subject Premises") and certain digital devices found at the Subject Premises for evidence, instrumentalities, and contraband relating to the offense. *See* ECF No. 1 at 1.[1] The government's application sought permission to compel certain individuals to unlock a device subject to seizure using the device's biometric features. *See* Application for a Search Warrant ¶ 17. Specifically, in the proposed warrant, the government requested authority for "law enforcement personnel . . . to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the [S]ubject [P]remises and

[1] The application and the proposed warrant were filed under seal under this case number. Because the investigation is ongoing and not fully known to all of the subjects of the investigation, the government respectfully requests the Court continue to maintain them under seal. The government will lodge courtesy copies of the sealed filings with Chambers.

reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this search warrant." *See* [Proposed] Search and Seizure Warrant at Attachment B, ¶ 7.

III. The Magistrate Judge's Order

On January 10, 2019, without the benefit of briefing from the government, the Court issued an unsealed order denying the application. ECF No. 1. The Magistrate Judge found "there are sufficient facts in the affidavit to believe that evidence of the crime will be found at the Subject Premises, so the Government has probable cause to conduct a lawful search, so long as it comports with the Fourth Amendment." *Id.* at 2. The Magistrate Judge further found probable cause to "seize those digital devices that law enforcement reasonably believes are owned and/or possessed by the two suspects named in the affidavit." *Id.* at 9. The Magistrate Judge nonetheless denied the application because it sought permission to compel certain individuals to unlock a device subject to seizure using the device's biometric features. The Magistrate Judge held, categorically, that "[t]he Government may not compel or otherwise utilize fingers, thumbs, facial recognition, optical/iris, or any other biometric feature to unlock electronic devices" on the ground that it would run afoul of the Fifth Amendment right against self-incrimination. *Id.* at 9. The Court further held that the proposed warrant would violate the Fourth Amendment. *Id.* at 3.

The Magistrate Judge's unsealed order gave notice to those in Oakland (and elsewhere) that the government was investigating use of a particular social media to commit extortion through particular means and was focused on a residence in Oakland. Within a week of the order, numerous news outlets published stories about it.[2]

[2] *E.g.*, Cyrus Farivar, *Feds forcing mass fingerprint unlocks is an "abuse of power," judge rules*, ARS TECHNICA, Jan. 14, 2019, https://arstechnica.com/tech-policy/2019/01/feds-forcing-mass-fingerprint-unlocks-is-an-abuse-of-power-judge-rules/; Thomas Brewster, *Feds Can't Force You to Unlock Your iPhone with Finger or Face, Judge Rules*, FORBES, Jan. 14, 2019, https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules; Rhett Jones, *Cops Can't Force People to Unlock Their Phones with Biometrics, Court Rules*, GIZMODO, Jan. 14, 2019, https://gizmodo.com/cops-cant-force-people-to-

On January 10, 2019, the day the Magistrate Judge's order was issued, in part to minimize the risk that evidence would be destroyed or moved, the government submitted a new search warrant application that, at the Magistrate Judge's request, omitted any reference to use of biometrics and sought authority to search only devices owned or controlled by two named individuals. The Magistrate Judge issued the new warrant on January 11, 2019. That new warrant has been executed.

JURISDICTION

Under the Federal Magistrates Act, 28 U.S.C. § 631, *et seq.*, magistrate judges have the authority to decide pretrial, non-dispositive matters. 28 U.S.C. § 636(b)(1)(A). Included within this pretrial authority is the issuance of search warrants. *See Gomez v. United States*, 490 U.S. 858, 868 n.16 (1989). Pursuant to the Federal Magistrates Act, "[a] judge of the court may reconsider any [non-dispositive] pretrial matter . . . where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law." 28 U.S.C. § 636(b)(1)(A); *see In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp.*, 212 F. Supp. 3d 1023, 1029 (D. Kan. 2016). "The magistrate's legal conclusions are reviewed de novo to determine whether they are contrary to law." *Perry v. Schwarzenegger*, 268 F.R.D. 344, 348 (N.D. Cal. 2010).

Notwithstanding the execution of the new warrant, a live controversy exists here. The Magistrate Judge's order involves a practice that directly affects the government, and the Magistrate Judge has made clear that she will not sign any search warrants that provide for use of biometrics to unlock electronic devices, as she believes use of biometrics violates both the Fourth and Fifth Amendments. Indeed, in the days immediately after she issued her order, she refused to sign other search warrant applications on the same grounds. This dispute is not moot merely because the

---

unlock-their-phones-with-biom-1831743969; Orin Kerr, *Search Warrants and Compelled Biometric Access to Phones*, VOLOKH CONSPIRACY, Jan. 15, 2019, https://reason.com/volokh/2019/01/15/search-warrants-and-compelled-biometric; Nicole Darrah, *Authorities can't force people to unlock technology with biometric features, US judge rules*, FOX NEWS, Jan. 15, 2019, https://www.foxnews.com/tech/us-authorities-cant-force-people-to-unlock-technology-with-fingerprint-facial-recognition-judge-rules; Marrian Zhou, *Police can't force you to unlock phone with Face ID or fingerprint, judge rules*, CNET, Jan. 15, 2019, https://www.cnet.com/news/police-cant-force-you-to-unlock-phone-with-face-id-or-fingerprint-judge-rules/; Mariella Moon, *US judge rules that feds can't force fingerprint or face phone unlocks*, ENGADGET, Jan. 15, 2019, https://www.engadget.com/2019/01/15/judge-biometrics-unlocking-rule/; Ian Lopez, *A California Judge May Have Changed the Conversation Around Biometrics Privacy Rights*, RECORDER, Jan. 17, 2019, https://www.law.com/therecorder/2019/01/17/a-california-judge-may-have-changed-the-conversation-around-biometrics-privacy-rights/.

government in this case resubmitted a new warrant application to the Magistrate Judge, at her request, after she refused to sign the original warrant. The government's action was purely one of necessity, resulting from the time sensitivity of an active investigation and from the Magistrate Judge's decision to publish her order publicly, which potentially put targets on notice of the government's investigation.

In general, a case is moot when the issues presented are no longer live or the parties lack a legally cognizable interest in the outcome. *County of Los Angeles v. Davis*, 440 U.S. 625, 631 (1979). The Supreme Court has recognized several well-established exceptions to the mootness doctrine, including if a dispute is "capable of repetition, yet evading review." *S. Pac. Terminal Co. v. ICC*, 219 U.S. 498, 515 (1911). A dispute is capable of repetition if "there [is] a reasonable expectation that the same complaining party would be subjected to the same action again," and it is likely to evade review if "the challenged action was in its duration too short to be fully litigated prior to its cessation or expiration." *Weinstein v. Bradford*, 423 U.S. 147, 149 (1975) (per curiam). That exception applies here. *See, e.g.*, *In re Search of Fair Finance*, 692 F.3d 424, 428–29 (6th Cir. 2012); *Phoenix Newspapers, Inc. v. U.S. Dist. Court*, 156 F.3d 940, 946 (9th Cir. 1998); *United States v. Brooklier*, 685 F.2d 1162, 1165 (9th Cir. 1982).

Even if this matter were moot and no exception applied, this Court would have authority to *vacate* the Magistrate Judge's order, if not to reverse it. *See Alvarez v. Smith*, 558 U.S. 87, 94–96 (2009); *see also United States v. Raddatz*, 447 U.S. 667, 681 (1980) ("Congress made clear that . . . the magistrate acts subsidiary and only in aid of the district court. . . . [T]he entire process takes place under the district court's total control and jurisdiction."). Given the important interests at stake, this Court should "offer guidance to" the Magistrate Judge and clarity to the government. *See In re United States*, 791 F.3d 945, 960–61 (9th Cir. 2015).

ARGUMENT

Compelling a person to provide a fingerprint or thumbprint as part of a search warrant, or holding a device in front of that person's face, violates neither the Fourth nor the Fifth Amendment.

///

///

///

I. The Fourth Amendment Permits the Use of Biometrics to Execute a Valid Search Warrant, But a Warrant Need Not Include Authorization to Use Biometrics.

The United States sought permission in its search warrant application to use individuals' hand digits and faces for the purpose of unlocking devices covered by the search warrant through the devices' biometric features, where those individuals were present at the execution of the search, the seizure occurred at the execution of the search, and where there was reasonable suspicion to believe the individuals used the device. The United States included this request not because it is required under the Fourth Amendment but because the Supreme Court has indicated that, while not required, making explicit to an authorizing court the means the government anticipates it will take to execute a search warrant is "preferable." *Dalia v. United States*, 441 U.S. 238, 258–59 & n.22 (1979) (internal quotation marks and citation omitted).

Dalia and *United States v. Grubbs*, 547 U.S. 90, 98 (2006), clearly explain that under the Fourth Amendment, search warrants need not specify the precise manner in which they are to be executed. Therefore, the United States need not specify how it intends to unlock electronic devices that a search warrant authorizes it to seize and search. The manner used by officers to execute a warrant "is subject to later judicial review as to its reasonableness." *Dalia*, 441 U.S. at 258.

Nor does the use of biometric data to preserve evidence covered by a search warrant require separate warrant authorization. *Dalia* also recognized that "in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant." *Dalia*, 441 U.S. at 257.

Moreover, there is no additional seizure of the persons beyond what is already authorized by a warrant. A valid premises search warrant implicitly carries with it the limited authority to briefly detain the occupants on, or in the immediate vicinity of, the premises while the search is being conducted. *Michigan v. Summers*, 452 U.S. 692, 705 (1981). The authority to detain carries with it the authority to "use reasonable force to effectuate detention." *Muehler v. Mena*, 544 U.S. 93, 98–99 (2005). This detention prevents flight in the event that incriminating evidence is found, minimizes the risk of harm to the officers, and facilitates orderly completion of the search. *Bailey v. United States*, 568 U.S. 186, 194

(2015); *Muehler*, 544 U.S. at 98 ("An officer's authority to detain incident to a search is categorical . . . .").

The government's use of biometric data to unlock devices that may otherwise be unlockable furthers both the avoidance of destruction of evidence and the orderly execution of a valid search warrant. Moreover, the slight movement of a subject's hands to take fingerprints or use a Face ID or similar technologies does not constitute a greater intrusion than the ability to direct a subject to a particular area or to handcuff a subject for the duration of the search; it is a reasonable use of force to effectuate the purposes of a limited detention set forth in *Summers*. *See Muehler*, 544 U.S. at 98–99. This practice stands in stark contrast to *Schmerber v. California*, where the Supreme Court held that although there was probable cause to arrest the defendant for driving an automobile while under the influence of intoxicating liquor, and the officer was therefore entitled to search him incident to arrest without a warrant, this did not authorize the officer to take a blood sample from the defendant. 384 U.S. 757, 771 (1966). The Supreme Court held that the blood draw involved an "intrusion[] beyond the body's surface" and implicated enhanced "interests in human dignity and privacy." *Id.* at 769–70.

Further, the Fourth Amendment does not protect what a person knowingly exposes to the public. *Katz v. United States*, 389 U.S. 347, 351 (1967); *United States v. Dionisio*, 410 U.S. 1, 14 (1973). And the Supreme Court has long held that "fingerprinting itself 'involves none of the probing into an individual's private life and thoughts that marks an interrogation or search.'" *Dionisio*, 410 U.S. at 15 (quoting *Davis v. Mississippi*, 394 U.S. 721, 727 (1969)). It is also "clear that a person has no expectation of privacy in a photograph of his face." *United States v. Emmett*, 321 F.3d 669, 672 (7th Cir. 2003) (cited by *Yezek v. Mitchell*, No. 05-C-3461 TEH, 2007 WL 61887, at *6 n.5 (N.D. Cal. Jan. 8, 2007)); *United States v. Doe*, 457 F.2d 895, 898 (2d Cir. 1972) (same); *cf. Maryland v. King*, 569 U.S. 435, 465–66 (2013) (holding that "taking and analyzing a cheek swab," like "fingerprinting and photographing," is "a legitimate police booking procedure that is reasonable under the Fourth Amendment").

The Magistrate Judge also expressed a concern about overbreadth, stating that "[t]he Government cannot be permitted to search and seize a mobile phone or other device that is on a non-suspect's person simply because they are present during an otherwise lawful search." ECF No. 1 at

3. But the United States sought no such authorization, and the Magistrate Judge's overbreadth concerns are unfounded. Rather, the proposed warrant would have authorized seizure of "evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 875" and "[c]omputers or storage media used as a means to commit [such] violations" and use of fingerprints and biometrics of individuals reasonably believed to use digital devices that the government is authorized to search. *See* [Proposed] Search and Seizure Warrant at Attachment B, ¶¶ 3, 4, & 7; *see also* Application for a Search Warrant, ¶¶ 7 & 7(i). The affidavit that the United States submitted in support of the search warrant here "established both probable cause to believe that a crime had been committed and that evidence of the crime would be found at the premises to be searched, including on the Subject Devices," so the warrant is not overbroad. *In re Search of [Redacted] Washington, DC*, 317 F. Supp. 3d 523, 527 & n.3 (D.D.C. 2018); *see United States v. Schesso*, 730 F.3d 1040, 1046–47 (9th Cir. 2013) (rejecting overbreadth challenge where search warrant permitted search and seizure of defendant's "entire computer system and associated digital storage devices," because "[t]he government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner," and noting that "[w]e have repeatedly found equally broad searches constitutional on similar or less evidence" (citing *United States v. Krupa*, 658 F.3d 1174, 1178 (9th Cir. 2011)); *United States v. Brobst*, 558 F.3d 982, 993–94 (9th Cir. 2009); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997))); *see also United States v. Adjani*, 452 F.3d 1140, 1148–49 (9th Cir. 2006) ("Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible.") (internal citations omitted).

II. The Fifth Amendment Permits the Government to Unlock a Device While Executing a Warranted Search by Using Biometrics.

"[T]here is a significant difference between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating." *United States v. Hubbell*, 530 U.S. 27, 34–35 (2000). Thus, "[t]o qualify for the Fifth Amendment privilege, a communication must be: (1) testimonial, (2) incriminating, and (3) compelled." *Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 189 (2004). Compelling a person to provide a fingerprint, or to face a

phone's screen, does not violate the Fifth Amendment, because even if that act is compelled *and* incriminating, it is not testimonial.

For decades, the Supreme Court has found numerous acts akin to the use of biometrics not to be testimonial and therefore not protected by the Fifth Amendment. "It has long been held that the compelled display of identifiable physical characteristics infringes no interest protected by the [Fifth Amendment] privilege against compulsory self-incrimination." *Dionisio*, 410 U.S. at 5–6. And the privilege "offers no protection against compulsion to submit to fingerprinting, photography, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture . . . [because] [n]one of these activities becomes testimonial within the scope of the privilege." *United States v. Wade*, 388 U.S. 218, 223 (1967) (quoting *Schmerber*, 384 U.S. at 764); *see also Hubbell*, 530 U.S. at 35; *Gilbert v. California*, 388 U.S. 263, 266–67 (1967). The Court has explained that compelled display of physical characteristics is not testimonial because a subject is "not required to disclose any knowledge he might have, or to speak his guilt." *Doe v. United States*, 487 U.S. 201, 211 (1988) (internal quotation marks omitted). The subject is not required "'to disclose the contents of his own mind.'" *Id.* (quoting *Curcio v. United States*, 354 U.S. 118 (1957)).

The Ninth Circuit has held the same: "[r]equests by the prosecution for . . . fingerprint evidence from a defendant or a suspect are not prohibited by the Fifth Amendment right against self-incrimination because such evidence is not testimonial in nature." *N. Mariana Islands v. Bowie*, 243 F.3d 1109, 1120 n.5 (9th Cir. 2001); *see also United States v. De Palma*, 414 F.2d 394, 397 (9th Cir. 1969) ("Identifying physical characteristics are not evidence of a testimonial nature."); *United States v. Sanudo-Duarte*, No. CR-14-01342-002-PHX-JAT, 2016 WL 126283, at *1 (D. Ariz. Jan. 12, 2016) (holding under Fourth and Fifth Amendments that defendant could be compelled to provide exemplar of his palm prints and that "palm prints are identifiable physical characteristics unprotected by the Fifth Amendment").

Under this well-established precedent, applying a fingerprint to an electronic device covered by a valid search warrant, or holding up a device in front of a subject's face, does not implicate the Fifth Amendment because law enforcement's action involves no compelled testimonial act by the subject. It does not require the subject to disclose the contents of his mind.

Contrary to precedent, the Magistrate Judge conflated the Fifth Amendment privilege's three distinct requirements: compelled, incriminating, and testimonial. The Magistrate Judge concluded that use of biometrics is testimonial because "a successful finger or thumb scan confirms ownership or control of the device, and, unlike fingerprints, the authentication of its contents cannot be reasonably refuted." ECF No. 1 at 6. But as the Supreme Court has made clear, the inquiry into whether an act is testimonial does not turn on whether an inference can be reasonably refuted, or indeed whether the act is incriminating.

That an act of unlocking a device may lead to incriminating evidence—including that the subject has control of a particular device—is irrelevant to the Fifth Amendment analysis. "If a compelled [action or] statement is not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence." *Doe*, 487 U.S. at 208–09 n.6 (1988) (internal quotation marks omitted); *see also Hubbell*, 530 U.S. at 35 (recognizing that "a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice," even if those acts may be incriminating) (citations omitted); *Fisher v. United States*, 425 U.S. 391, 411 (1976) ("[A]lthough the [handwriting] exemplar may be incriminating to the accused and although he is compelled to furnish it, his Fifth Amendment privilege is not violated because nothing he has said or done is deemed to be sufficiently testimonial for purposes of the privilege.").[3]

In addition to contravening Supreme Court and Ninth Circuit precedent, the Magistrate Judge's order conflicts with decisions of lower courts—decisions that the Magistrate Judge did not acknowledge, let alone distinguish.

Most strikingly, while relying on the decision of a magistrate in the Northern District of Illinois, *see* ECF No. 1 at 6 (citing *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill.

[3] Because law enforcement's compelled use of a subject's fingerprint or face is not a testimonial act by the subject, the Magistrate Judge had no need to analyze the "foregone conclusion" doctrine, *see Fisher*, 425 U.S. at 411, and the United States does not invoke that doctrine here. The United States notes, however, that the Magistrate Judge's conclusion that the foregone conclusion doctrine cannot apply to electronic devices because law enforcement cannot anticipate the "full contents" of the devices, *see* ECF No. 1 at 8, is squarely contrary to a recent district court opinion in this District. *See United States v. Spencer*, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018) (holding that in order to invoke the foregone conclusion doctrine in the context of compelled decryption, "the government need only show it is a foregone conclusion that [the subject] has the ability to decrypt the devices"). The Magistrate Judge did not cite this opinion.

2017)), the Magistrate Judge failed to cite a subsequent contrary decision by a U.S. district judge on the same court: *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d 800 (N.D. Ill. 2017).

In that more recent decision, the district court reversed a magistrate judge and held that no Fifth Amendment testimonial act occurs when agents press a subject's fingers against a Touch ID sensor on an iPhone, because "the government agents will pick the fingers to be pressed on the Touch ID sensor, so there is no need to engage the thought process of any of the residents at all in effectuating the seizure," and applying the fingerprint to the sensor "is simply the seizure of a physical characteristic, and the fingerprint by itself does not communicate anything." *Id.* at 803–04. The district court distinguished the Supreme Court's *Hubbell* decision because there, "the act of producing the records *inherently* represented communications from the defendant," but "[n]ot so with the fingerprint seizure":

> The government chooses the finger to apply to the sensor, and thus obtains the physical characteristic—all without need for the person to put any thought at all into the seizure. . . . *[T]he person's performance of the compelled act is not an act of communication by that person. Indeed, the person can be asleep—and thus by definition not communicating anything—when a seizure of this sort is effectuated.* If anything, handwriting and voice exemplars require a person to engage more mental processes than simply providing a finger for application to the Touch ID sensor. And if anything, handwriting and voice exemplars contain more implicit admissions than a fingerprint, namely, that "I can write and this is my handwriting," or "this is my voice and this is how I pronounce this word."

Id. at 804 (citations omitted) (emphasis added). The court in that case also agreed with the government that whether "the physical characteristic yields incriminating information is *not* the dividing line between whether a compelled act comprises testimonial communication or not," and that the Supreme Court in *Doe* rejected the conflation of those two issues. *Id.* at 805. "That distinction—between whether an act is testimonial versus whether the act is incriminating—explains why physical characteristics, like fingerprints, blood samples, handwriting, and so on are not protected by the privilege even though they often are highly incriminating. . . . If the act does not *inherently* contain a communication from the person, then no testimony has been obtained from the person." *Id.*

The Magistrate Judge also did not acknowledge another recent published decision that undermined her reasoning: *In re Search of [Redacted] Washington, DC*, 317 F. Supp. 3d 523 (D.D.C.

2018). There, the district court held that "the compelled use of the Subject's biometric features" is not testimonial under the Fifth Amendment:

> As other courts have recognized, there will be no revelation of the contents of the Subject's mind with the procedure proposed by the government for collection of the Subject's biometric features. Rather, "[t]he government chooses the finger to apply to the sensor, and thus obtains the physical characteristic—all without the need for the person to put any thought at all into the seizure."

Id. at 535–36 (collecting cases) (quoting *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d at 804). The district court went on to conclude that "the use of the fingerprint is much more like the government's compelled use of other 'physical characteristics' of criminal suspects that courts have found non-testimonial even when they are used for investigatory purposes rather than solely for identification." *Id.* at 536 (citations omitted). As the district court observed, "The 'distinction which has emerged' as a 'helpful framework for analysis' is that the Fifth Amendment 'privilege is a bar against compelling communication or testimony, but that compulsion which makes a suspect or accused the source of real or physical evidence does not violate it.'" *Id.* (quoting *Schmerber*, 384 U.S. at 764) (internal quotation marks omitted). Again, the Magistrate Judge made no effort to grapple with this well-reasoned adverse authority.

Nor did the Magistrate Judge acknowledge adverse state-court authority, such as *Minnesota v. Diamond*, 905 N.W.2d 870, 876 (Minn.) ("[Defendant's] act of providing a fingerprint to the police was not testimonial because the act did not reveal the contents of [his] mind."), *cert. denied*, 138 S. Ct. 2003 (2018). And while the Magistrate Judge did cite *Commonwealth v. Baust*, 89 Va. Cir. 267, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014)—a case cited by the U.S. District Court for the District of Columbia in the decision discussed above—the Magistrate Judge ignored the Virginia court's holding that law enforcement could use a subject's fingerprint to unlock a phone, and that "[t]he fingerprint . . . does not require the witness to divulge anything through his mental processes." The Magistrate Judge cited *Baust* only for the proposition that giving up a *passcode* is testimonial. *See* ECF No. 1 at 4.

Finally, the Magistrate Judge's "functional equivalence" theory—under which the government may not use biometrics such as a face or fingerprint to unlock a device because biometrics are the functional equivalent of a passcode—also contravenes Supreme Court case law. A key to a safe is the

functional equivalent of a combination. Yet the Supreme Court, at least in dicta, has distinguished compelling the disclosure of a key from compelling the disclosure of a combination. *See Doe*, 487 U.S. at 210 n.9; *Hubbell*, 530 U.S. at 43; *In re Search of [Redacted] Washington, DC*, 317 F. Supp. 3d at 535–36.

CONCLUSION

The Magistrate Judge's order—issued without the benefit of any briefing—is contrary to law and should be reversed or vacated. The Magistrate Judge's constitutional analysis is fundamentally flawed. And the order, if allowed to stand, will hinder the government's ability to conduct lawful searches pursuant to valid warrants. For these reasons, the Court should overrule or vacate the order.

Dated: January 23, 2019

Respectfully submitted,

DAVID L. ANDERSON
United States Attorney

/s/
ROBERT S. LEACH
JONAS LERMAN
Assistant United States Attorneys